ISO31000やCOSO-ERMの改訂からみる今後の企業RM

2018年10月6日

長井　健人
MS&ADインターリスク総研株式会社

ISO31000の改訂

- “ISO31000：Risk management –Guidelines”が2018年2月に改訂(第2版)
- 改訂の趣旨：
  - 組織との統合とリーダーの役割と責任に重点
  - より単純な表現を使用して明瞭さを重視
  - 「リスク：目的に対する不確実性の影響」を強調
- 主要な変更点
  - 成功のための重要な基準であるリスクマネジメントの原則の見直し
  - 組織のガバナンスから始まるすべての組織活動にリスクマネジメントが確実に統合されるようにする、トップマネジメントによるリーダーシップの強調
  - プロセスの各段階におけるプロセス要素、活動、対策・制御の改訂に関する新しい経験、知識、分析を引き出すことに留意した、リスクマネジメントの反復性の重視
  - 定期的に外部環境からのフィードバックを反映し、複数のニーズや状況に適合させ易くするために、オープンなシステムモデルを維持することに重点を置いてコンテンツを合理化

出典：The new ISO 31000 keeps risk management simple（By Sandrine Tranchard on 15 February 2018）
https://www.iso.org/news/ref2263.html

2009年版と2018年版の目次比較

2009	2018
序文	序文
1適用範囲	1適用範囲
	2引用規格
2用語及び定義	3用語及び定義
3原則	4原則
4枠組み	5枠組み
4.1一般	5.1一般
4.2指令及びコミットメント	5.2リーダーシップ及びコミットメント
	5.3統合
4.3リスクの運用管理のための枠組みの設計	5.4設計
4.3.1組織及び組織の状況の理解	5.4.1組織及び組織の状況の理解
4.3.2リスクマネジメント方針の確定	5.4.2 リスクマネジメントに関するコミットメント の明示
4.3.3アカウンタビリティ	5.4.3組織の役割, 権限, 責任及びアカウンタビリティの割当て
4.3.4組織のプロセスへの統合	
4.3.5資源	5.4.4資源の配分
4.3.6内部のコミュニケーション及び報告の仕組みの確定	5.4.5コミュニケーション及び協議の確立
4.3.7外部のコミュニケーション及び報告の仕組みの確定	
4.4リスクマネジメントの実践	5.5実施
4.4.1リスクの運用管理のための枠組みの実践	
4.4.2リスクマネジメントプロセスの実践	
4.5枠組みのモニタリング及びレビュー	5.6評価
4.6枠組みの継続的改善	5.7改善
	5.7.1 適応
	5.7.2 継続的改善

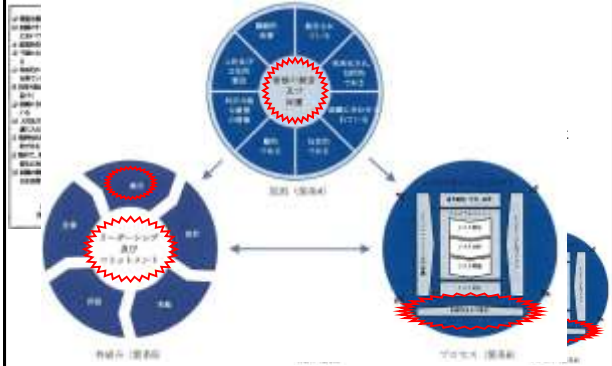
2009年版と2018年版の目次比較

2009	2018
5プロセス	6プロセス
5.1一般	6.1一般
5.2コミュニケーション及び協議	6.2コミュニケーション及び協議
5.3組織の状況の確定	6.3適用範囲,組織の状況及び基準
5.3.1一般	6.3.1一般
5.3.2外部状況の確定	6.3.2 適用範囲の決定
5.3.3内部状況の確定	6.3.3 外部及び内部の状況
5.3.4リスクマネジメントプロセスの状況の確定	
5.3.5リスク基準の決定	6.3.4リスク基準の決定
5.4リスクアセスメント	6.4リスクアセスメント
5.4.1一般	6.4.1一般
5.4.2リスク特定	6.4.2リスク特定
5.4.3リスク分析	6.4.3リスク分析
5.4.4リスク評価	6.4.4リスク評価
5.5リスク対応	6.5リスク対応
5.5.1一般	6.5.1一般
5.5.2リスク対応の選択肢の選定	6.5.2リスク対応の選択肢の選定
5.5.3リスク対応計画の準備及び実施	6.5.3リスク対応計画の準備及び実施
5.6モニタリング及びレビュー	6.6モニタリング及びレビュー
5.7リスクマネジメントプロセスの記録作成	6.7記録作成及び報告

原則～リスク対応：
2009年　15ページ
2018年　14ページ

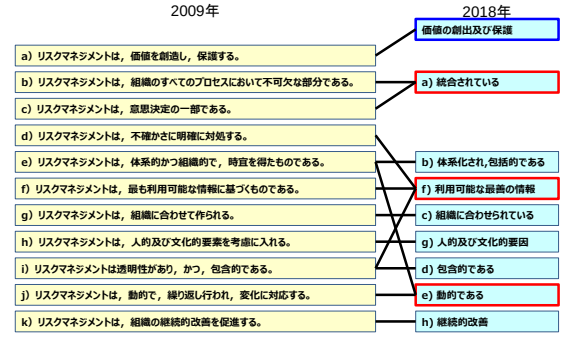
全体像　（原則⇔枠組み⇔プロセス）

- 原則と枠組みが大きく変更されている。



4　原則

- リスクマネジメントの目的は、“（組織の）価値の創造および保護”



5.2 リーダーシップ及びコミットメント

- トップマネジメントに加えて監督機関の概念を導入
- リスクマネジメントを組織のすべての活動に統合することを強調

  - トップマネジメント及び監督機関(該当する場合)は,リスクマネジメントが組織のすべての活動に統合されることを確実にすることが望ましい。また,次の事項を通じてリーダーシップ及びコミットメントを示すことが望ましい:
    - 枠組みのすべての構成要素を組織に合わせ,実施する;
    - リスクマネジメントの取組み方,計画又は活動方針を確定する記述又は方針を公表する;
    - 必要な資源がリスクのマネジメントを行うことに配分されることを確実にする;
    - 権限,責任及びアカウンタビリティを,組織内の適切な階層に割り当てる。
  - トップマネジメントはリスクのマネジメントを行うことに責任を負い,監督機関はリスクマネジメントを監視する責任を負う。

5.3 統合

- リスクマネジメントと組織の統合とは、組織のあらゆる部分における組織全員でのリスクのマネジメント
- リスクマネジメントは組織統治と不可分。組織統治は組織の目的達成のため。

  - リスクマネジメントの統合は，組織の体制及び状況の理解にかかっている。体制は，組織の意図，目標及び複雑さによって異なる。リスクは，組織の体制のあらゆる部分でマネジメントされる。組織の全員が，リスクのマネジメントを行うことの責任を負っている。
  - 組織統治は，組織の意図を達成するために，組織の方向性，組織の外部関係及び内部関係，並びにプロセス及び方策を導く。経営体制は，組織統治の方向性を，望ましいレベルの持続可能なパフォーマンス及び長期的な継続性を達成するために必要な戦略及び関連する目的へと転換する。組織内部におけるリスクマネジメントのアカウンタビリティ及び監視の役割の決定は，組織の統治と不可分である。
  - リスクマネジメントと組織の統合は動的で，反復的なプロセスである。この統合は，組織の必要性及び文化に合わせることが望ましい。リスクマネジメントは，組織の意図，組織統治，リーダーシップ及びコミットメント，戦略，目的及び業務活動の一部となり，これらと分離していないことが望ましい。

ISO31000:2018の活用に際して

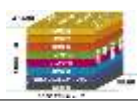
- リスクマネジメントの組織における位置づけが、2009年版に比べて一層明確になっている。
  - 「損失を生じる可能性のある事象の発見とその対処のためのツール」という理解で2018年版をみると不親切なガイドライン
  - リスク特定やリスク分析、リスク評価においては、手順的な記載は少なく、考慮事項についての記載にとどまっている
- リスクマネジメントの目的は、組織の価値の創出および保護
  - 組織のパフォーマンスを改善し、イノベーションを促進し、組織の目的を支援する
  - 組織が目的を達成する上での不確実性を認識し、それに対応していく際に考慮すべき事項は何かという観点で読む・・・(手順を示すようなHow toではない)
  - 不確実性を認識したり対応したりする際の手法を拘束的に定めるものではない。
    ⇒手法はそれぞれの組織で適した方法を採用すればよい。

COSO-ERMの改訂

- COSO-ERMの改訂版が2017年9月に公表された。
  - Enterprise Risk Management-Integrating with Strategy and Performance
    (全社的リスクマネジメント　戦略及びパフォーマンスとの統合)
- 「2004年版　全社的リスクマネジメント　統合的フレームワーク」の反省
  - × ERMは機能や部門である
  - × ERMとはリスクを一覧化することである
  - × ERMとは内部統制を対象とすることである
  - × ERMはチェックリストである
  - × ERMは中小規模の組織には適用できない　　等々の誤解を受けてしまった
  - 日本の企業の多くが上記のように認識していると思われる

COSO-ERM:2004年版と2017年版

	2004年版	2017年版
リスクの定義	リスクとは目的達成を阻害する影響を及ぼす事象が生じる可能性 事業機会とは目的達成にプラスの影響を及ぼす事象が生じる可能性	事象が発生し、戦略と事業目的の達成に影響を及ぼす可能性
リスクマネジメントの定義	組織内の全ての者によって遂行され、事業体の戦略策定に適用され、事業体全体にわたって適用され、事業目的の達成に関する合理的な保証を与えるために事業体に影響を及ぼす発生可能な事象を識別し、事業体のリスク選好に応じてリスクの管理が実施できるように設計された一つのプロセス	組織が価値を創造し、維持し、および実現する過程において、リスクを管理するために依拠する、戦略策定ならびにパフォーマンスと統合されたカルチャー、能力、実務
構成要素	8つの構成要素 ①内部環境、 ②目的の設定 ③事象の識別 ④リスクの評価 ⑤リスクへの対応 ⑥統制活動 ⑦情報と伝達 ⑧モニタリング	5つの構成要素 ①ガバナンスとカルチャー ②戦略と目標設定 ③パフォーマンス（実行） ④レビューと見直し ⑤情報、伝達と報告



COSO-ERM:2004年版と2017年版

2017年版 (144頁)

8つの構成要素	原則
①内部環境 (12頁)	リスクマネジメントの考え方
	リスク選好
	取締役会
	誠実性と倫理観
	専門能力に対するコミットメント
	組織構造
	権限と責任の付与
	人的資源に関する基準
②目的の設定 (9頁)	戦略目的
	関連目的
	選択した目的
	リスク選好
	リスク許容度
③事象の識別 (10頁)	事象
	影響を及ぼす要因
	事象識別の手法
	相互依存
	リスクと事業機会の区別
④リスクの評価 (9頁)	固有リスクと残余リスク
	発生可能性と影響度の推定
	評価手法
	事象間の関係
⑤リスクへの対応 (8頁)	選択し得る対応策の評価
	選択された対応策
	ポートフォリオの視点
⑥統制活動 (10頁)	リスク対応策との統合
	統制活動のタイプ
	方針と手続
⑦情報と伝達 (11頁)	情報システムに対する統制手続
	情報
	伝達
⑧モニタリング (10頁)	継続的モニタリング活動
	独立的評価
	欠陥の報告

2004年版 (79頁)

2017年版 原則	5つ構成要素
1. 取締役会によるリスク監視を行う 2. 業務構造を確立する 3. 望ましいカルチャーを定義づける **4. コアバリューに対するコミットメントを表明する** 5. 有能な人材を惹きつけ、育成し、保持する	①ガバナンスとカルチャー（30頁）
6. 事業環境を分析する **7. リスク選好を定義する** 8. 代替戦略を評価する 9. 事業目標を組み立てる	②戦略と目標設定（32頁）
10. リスクを識別する **11. リスクの重大度を評価する** **12. リスクの優先順位づけをする** 13. リスク対応を実施する 14. ポートフォリオの視点を策定する	③パフォーマンス（実行）（46頁）
15. 重大な変化を評価する 16. リスクとパフォーマンスをレビューする 17. 全社的リスクマネジメントの改善を追求する	④レビューと見直し（13頁）
18. 情報とテクノロジーを有効活用する 19. リスク情報を伝達する 20. リスク、カルチャーおよびパフォーマンスについて報告する	⑤情報、伝達と報告（23頁）

読みやすく、内容も濃くなっている。

原則 4. コアバリューに対するコミットメントを表明する

- 組織は事業体のコアバリューに対するコミットメントを表明する。
  - コアバリュー: 組織の行動に影響を与える、善悪や許容できること/できないことに関する事業体の信条と理念
- 内容:

組織全体にコアバリューを反映させる	●事業体のコアバリューを組織全体に理解させる→全社リスクマネジメントの基本 ●コアバリューは、組織全体で行われる行動と意思決定に反映される。
リスクを認知するカルチャーを奨励する	●経営者は、望ましいカルチャーを作るために必要なことを定める。 ●リスクを認知するカルチャーを奨励していく方法・・・・具体的方法を列挙
説明責任を果たしている	●取締役会は、最高経営責任者に対して、全社的リスクマネジメントの実務を確立して事業体が直面するリスクの管理、および事業体の戦略と事業目標の達成に必要な能力について、最終的な説明責任を持たせる。
自らに説明責任を持たせる	●各階層においてコアバリューとカルチャーに沿った望ましい行動の実施について説明責任が課され、その実施状況が評価される。
開かれたコミュニケーションを維持し、不利益な扱いをしない	●リスクとリスクテイクへの期待についての開かれたコミュニケーションと透明性を確保することは、経営者の責任 ●経営者は、リスクの管理は全員の日々の責任の一部であり、それは事業体の成功と存続に不可欠であるということを明確に伝える

原則 6. 事業環境を分析する

- 組織は、リスクプロファイルに対する事業環境の潜在的影響を検討する。
  - リスクプロファイル:組織の戦略あるいは事業目標に対するパフォーマンスレベルとリスク想定量との関係を示したもの。(横軸にパフォーマンス、縦軸に想定リスク量をとった図上に表現された曲線)
  - リスクプロファイルは、事業体が抱えるリスク総量、リスクの分布状況、リスクのカテゴリー等の情報を提供する。
- 内容

事業環境を理解する	●組織は戦略を作成する際、事業環境を検討する ●事業環境:組織の現在および将来の戦略と事業目標に与えるトレンド、関連性、およびその他の要因をいう
外部環境と外部のステークホルダーを検討する	●外部環境:政治、経済、社会、技術、法規、環境の6分類(PESTLE) ●外部ステークホルダー:事業体の影響を受ける(顧客、取引先等)、事業体の事業環境に直接影響する(政府、規制当局等)、事業体の評判、ブランド、信用に影響する(地域社会、利害関係者等)すべての者
内部環境と内部のステークホルダーを検討する	●内部環境:事業体の戦略および事業目標の達成に対する能力に影響するすべてのもの(資本、人材、プロセス、テクノロジー) ●内部ステークホルダー:取締役会、経営者、その他の職員等事業体内で業務を行い、組織に直接影響を与えている人々
事業環境がどのようにリスクプロファイルに影響を及ぼすか	●過去や現在のパフォーマンスを検討することにより、リスクプロファイルを形成するために活用できる有用な情報(傾向、種々の要因とリスクプロファイルとの関連性等)を知ることができる ●過去、現在のそれぞれの関連要因が未来においてどのようになっていくかを検討することによって、今後組織が進もうとしている方向と関連して、リスクプロファイルがどのように進化していくかを検討することができる

7. リスク選好を定義する

- 組織は、価値の創造、維持、実現の観点からリスク選好を定義する。
  - リスク選好:組織が価値追及において受け入れる、幅広いリスクの種類と量。
- 内容

リスク選好を適用する	●意思決定方法に関わらず、組織は、リスク選考について事前に理解しておく必要がある ●リスク選好の表現には、量的・質的の両方ありうるが、事業体のカルチャーを反映したものでなければならない。 ●組織は、一般的にリスク選好をリスクキャパシティ(受け入れ可能なリスク量)の範囲内にとどまるように努力しなければならない。
リスク選好を決定する	●すべての事業体に適用可能な"標準的な"あるいは"正しい"リスク選考はない。 ●リスク選好は、パフォーマンスに対する追加的な制約ではなく、事業体のリスクプロファイルを明確にするための能動的なアプローチとして位置づけられ、認識されるべきである。 ●経営者がリスク選好を決定する場合には、何よりも、リスクプロファイル、リスクキャパシティ、自組織のリスクマネジメント能力と成熟度を検討する。
リスク選好を明確に表現する	●リスク選好は、取締役会の承認を経て経営者によって事業体内に伝えられ、全体に周知される。 ●リスク選好を広く周知することは、すべての意思決定者がリスク選好の範囲内で事業を行わなければならないことを理解し、すべての業務がリスク選好に沿うようになされるようにするために重要。
リスク選好を活用する	●リスク選好は、全社レベルと個別業務ユニットレベルのいずれでも、いかに経営資源を配分するかについて指針を提供する。 ●リスク選好は、業務の実施における意思決定に組み込まれる。 ●リスク選好は、意思決定におけるアプローチの一部であり、リスク選好を意思決定に組み込む場合には、関連する周辺の実務も含めた実務上の整合性を確保する必要がある。

11. リスクの重大度を評価する

- 組織は、11. リスクの重大度を評価する
- 内容

リスクを評価する	●事業体のリスク一覧表で識別されたリスクは、事業体の戦略および事業目標の達成に対するそれぞれのリスクの重大度を理解するために評価される
事業体における異なる階層での重大度を評価する	●リスクの重大度は、影響を受ける可能性のある事業目標に沿って、複数の階層(部門、機能及び業務ユニット等)で評価される。
重大度の測定基準の選択	●経営者は、リスクの重大度を評価する測定基準を選択する。 ●測定基準は、事業体の規模、性質及び複雑さ、そのリスク選好と整合する。 ●測定基準は、リスク、戦略、事業目標と結びつかなければならない。 ●事業体の各階層では、異なる閾値を使用することもできる。 ●経営者は、適切なリスク対応の選択、資源の配分を行うために様々なリスクの重大度を決定する。例えば、影響度、発生可能性、持続性、速度、複雑性 ●リスクを評価する際の時間軸は、それに関連する戦略および事業目標に使用したものと同一であるべきである。
評価アプローチ	●リスク評価のアプローチは、定性的、定量的、またはその両方で行われる。
固有リスク、M目標リスク及び残余リスク	●リスク評価の一部として、固有リスク、ターゲットとする残余リスク、実際の残余リスクを考慮する。
評価結果を描写する	●ヒートマップ(リスクマップ、リスクマトリックス)
再評価の契機を識別する	●契機は、事業環境の変化やリスク選好の変化などがある。
評価におけるバイアス	●経営者は、リスク評価活動におけるバイアスの影響を識別し、軽減させる。

12. リスクの優先順位づけをする

- 組織は、リスク対応選択の基礎として、リスクの優先順位づけを行う。
- 内容

基準を設定する	●組織はリスク対応に関する意思決定および資源の割り当てを最適化するためにリスクの優先順位づけを行う。 ●優先順位づけは、同意された基準を適用することで決定される。(この基準は、リスクの重大度を評価する際の基準としても使用される) 例えば、事業体のリスクへの対応能力、リスクの範囲と性質(例えば相互依存性の高いリスク)、影響伝播の速度、影響の出る期間、事業体の回復能力等
リスク選好を活用したリスクの優先順位づけ	●経営者は、リスクの優先順位づけの際にリスク選好と比較すべきである。
すべての階層における優先順位づけ	●事業体のすべての階層においてリスクの優先順位づけが行われる。 ●組織は、どのリスクの責任を負っているのか、それを管理する責任者は誰か等、その階層に応じて優先度を割り当てる。 ●リスクオーナー(リスク責任者)は、リスクを効果的に管理するための実行責任と説明責任に基づきリスクを優先順位づけする権限を持たなければならない。 ●リスクオーナー(リスク責任者)は、事業目標及びパフォーマンス目標の範囲において、適切なリスク対応を選択し適用するために割り当てた優先順位を利用する責任がある。 ●多くの場合、リスク責任者とリスク対応の責任者は異なる。

COSO-ERM:2017の活用に際して

- リスクマネジメントが、戦略と事業目的の達成を確実性を高めるものであること及びその為の道筋が、一層明確かつ具体的に示されるようになっている。
  - リスクマネジメントは、プロセスではなく、「リスクを管理するために依拠する、戦略策定ならびにパフォーマンスと統合されたカルチャー、能力、実務」という基本概念に沿った記述となっており、実務的に非常に使いやすいものとなっている。
  - ISO31000と似たプロセスで記載されつつも、リスクマネジメントは「戦略と事業目的の達成」のためのものであることを、全編において強調することで、リスクマネジメントが機能や部門に矮小化されることを予防している。
- 組織や役割を立体的に捉えている。
  - 事業体が部署や階層、責任分担(役割)などで構成されていることを認識したリスクマネジメントのあり方を提示している。
    - リスク選好は、全社レベルと個別業務ユニットレベルのいずれでも、いかに経営資源を配分するかについて指針を提供する。
    - リスクの重大度は、影響を受ける可能性のある事業目標に沿って、複数の階層(部門、機能及び業務ユニット等)で評価される。
  - リスク対応における責任分担を提示している。
    - リスクオーナー(リスク責任者)は、リスクを効果的に管理するための実行責任と説明責任に基づきリスクを優先順位づけする権限を持たなければならない。
    - 多くの場合、リスク責任者とリスク対応の責任者は異なる。

これからの企業リスクマネジメントに求められる事項

- リスクマネジメントを、「組織の価値の創造を支援する」ものと位置付けるとともに、そのアウトプットを明確にしていくことが求められている。
  - CSRやSDGs、コーポレートガバナンスコード、会社法
- そのための課題として、ISOやCOSOの新版では、以下を提示している。
  - リスクマネジメントを組織やその文化、活動と一体のものとする
    - 例えば、リスクマネジメントの推進体制を全社的に定める
    - 例えば、リスクマネジメントの活動を全社的活動や年間計画に組み込む
    - 例えば、階層別、部署別のリスク優先順位も明確にする
  - 組織の目的や事業目標と整合したリスクマネジメントの取組みとする
    - 例えば、社是や事業目標とリスクの洗い出し、分析・評価の基準を整合させる

これからの企業リスクマネジメントに求められる事項

（続き）

- リスク対策の立案、実施まで行う
  - 例えば、リスク一覧作りで終わらない
  - 例えば、リスク低減目標，リスク低減計画、モニタリング計画を明確にする
- リスクマネジメントの取組みを評価する
  - 例えば、評価体制や評価の考え方を明確にする
  - 例えば、経営層が評価結果をレビューし、次ステージの課題を明確に示す

ご清聴、ありがとうございます。

長井健人
MS&ADインターリスク総研株式会社